IN THE CLAIMS

Claims 1-17 (Cancelled).

18. (Currently Amended) An optically readable data storage medium, comprising an optically readable substrate having a data pattern and a set of optically readable characteristics which are randomly determined by a non-deterministic physical manufacturing process, further comprising a recorded self-authenticating cryptographic hash of identifications generated from a reading of the random optically readable characteristics and the data pattern associated with the data storage medium, the data pattern and the optically readable characteristics being adapted to be readable by a common imaging system, wherein the data storage medium is resistant to reproduction and alteration of the data pattern can be detected.

19. (Previously Presented) The storage medium according to claim 18, wherein the data storage medium comprises an identification card.

20. (Currently Amended) The storage medium according to claim 18, wherein the data pattern is molded into the data storage medium and the self-authenticating cryptographic hash are formed as a pattern on a surface of the medium in a common plane with the molded data pattern.

21. (Currently Amended) A data storage disk, comprising a graphic-bearing surface, a code printed on the graphic bearing surface, and an ascertainable pattern formed during a physical non-deterministic manufacturing process formed on the disk, wherein the printed code provides cryptographic self authentication hash for the disk generated based on ascertainment of the ascertainable pattern, the printed code and the ascertainable pattern being adapted to be readable by a common imaging system, wherein the data storage disk is resistant to reproduction.

22. (Withdrawn-Currently Amended) A system for reading an optically readable data storage medium having a common imaging system for authentication and data retrieval, comprising:

an optically readable substrate having a data pattern and a set of optically readable characteristics which are randomly determined by a non-deterministic physical manufacturing process, further comprising a recorded self-authenticating cryptographic hash of identifications generated from a reading of the random optically readable characteristics, and the data pattern, associated with the data storage medium; and

an encoded optical disk reader, comprising:

(a) an optical sensor having a common optical path for reading the recorded self-authenticating cryptographic hash of identifications, the data pattern, and the set of optically readable characteristics from the disk;

(b) a non-deterministic characteristic analyzer for analyzing the set of optically readable characteristics; and

(c) an authenticator, authenticating the disk based on an output of the non-deterministic characteristic analyzer and the recorded self-authenticating cryptographic hash of identifications, wherein the optically readable substrate is resistant to reproduction and alteration of the data pattern can be detected.

23. (Withdrawn) The system according to claim 22, wherein the optical sensor reads an optical encoding of the disk and the set of optically readable characteristics.

24. (Withdrawn) The system according to claim 22, wherein the optical sensor is distinct from an optical sensor which reads an optical encoding of the disk while sharing the common optical path.

25. (Withdrawn) The data storage disk according to claim 22, wherein the set of optically readable characteristics comprises a random reading defect of the disk.

26. (Withdrawn) The data storage disk according to claim 22, wherein the set of optically readable characteristics comprises a dye pattern on the disk.

27. (Withdrawn) The data storage disk according to claim 22, wherein the set of optically readable characteristics comprises a random distribution of fibers disposed on the disk.

28. (Withdrawn) The data storage disk according to claim 22, wherein the optical sensor reads a self-authentication code from the disk.

Claims 29-40 (Cancelled)

41. (Currently Amended) The system according to claim 46, wherein the optically readable substrate comprises a self-authenticating sealing tape, the tape further comprising a seal tamper indicator, the data pattern comprises a plurality of unique identification portions of the tape, periodically disposed along a length thereof, wherein a recorded self-authenticating cryptographic hash of identifications is disposed proximate to a respective unique identification portion.

42. (Previously Presented) The system according to claim 41, wherein the optically readable characteristics comprise a pattern selected from the group consisting of a random dye pattern and a random fiber pattern.

43. (Currently Amended) An optically readable data storage medium, comprising: an adhesive-backed flexible substrate; periodically disposed sets of optically readable data patterns on said substrate; regions of said substrate having optically readable characteristics which are randomly determined by a non-deterministic physical manufacturing process proximate to a respective data pattern; and periodically disposed sets of recorded self-authenticating cryptographic hashes, each respective self-authenticating cryptographic hash being ~~formed from~~ generated based on a reading of a respective data pattern and characteristics of a respective region, wherein the data storage medium is resistant to reproduction and alteration of the data pattern can be detected.

44. (Previously Presented) The optically readable data storage medium according to claim 43, wherein the optically readable characteristics comprise a random dye pattern

45. (Previously Presented) The optically readable data storage medium according to claim 43, wherein the optically readable characteristics comprise a random fiber pattern.

46. (Currently Amended) An optically readable data storage medium, comprising an optically readable substrate having a data pattern and a set of optically readable characteristics which are randomly determined by a non-deterministic physical manufacturing process, further comprising a self-authenticating cryptographically processed set of identifications generated from a reading of the random optically readable characteristics, and the data pattern, associated with the data storage medium, the data pattern and the optically readable characteristics being adapted to be readable by a common imaging system, wherein the data storage medium is resistant to reproduction and alteration of the data pattern can be detected.

47. (Currently Amended) The optically readable data storage medium according to claim 46, wherein said self-authenticating cryptographically processed set of identifications comprises a cryptographic hash.

48. (Currently Amended) The optically readable data storage medium according to claim 46, wherein said self-authenticating cryptographically processed set of identifications comprises a digital signature.

49. (Currently Amended) The optically readable data storage medium according to claim 46, wherein said self-authenticating cryptographically processed set of identifications is encrypted using a public-key private key technique.

50. (Previously Presented) The optically readable data storage medium according to claim 46, wherein said optically readable characteristics comprise a fluorescence pattern.

51. (Previously Presented) The optically readable data storage medium according to claim 46, wherein said optically readable characteristics comprise a polarization pattern.

52. (Previously Presented) The optically readable data storage medium according to claim 46, wherein said optically readable characteristics comprise a random fiber pattern.

53. (Currently Amended) The optically readable data storage medium according to claim 46, in combination with an authentication device, said authentication device comprising:

(a) an illumination source having an output adapted for exciting fluorescence;

(d) an optical imaging sensor, for sensing a pattern of fluorescence; and

(e) a processor for analyzing said pattern of fluorescence as said set of optically readable characteristics which are randomly determined by a non-deterministic physical manufacturing process, to determine a correspondence thereof with said self-authenticating cryptographically processed set of identifications of the random optically readable characteristics and the data pattern associated with the data storage medium.

54. (Previously Presented) The optically readable data storage medium according to claim 53, wherein said set of optically readable characteristics which are randomly determined by a non-deterministic physical manufacturing process comprise a non-deterministic optical polarization pattern.

55. (Previously Presented) The optically readable data storage medium according to claim 53, wherein said set of optically readable characteristics which are randomly determined by a non-deterministic physical manufacturing process comprise a non-deterministic optical fluorescent polarization pattern, wherein said illumination source excites a fluorescence of said pattern, and said optical imaging sensor determines a polarized fluorescent optical pattern.

56. (Previously Presented) The optically readable data storage medium according to claim 53, wherein said set of optically readable characteristics which are randomly determined by a non-deterministic physical manufacturing process comprise a non-deterministic optical polarization pattern, wherein said optical imaging sensor determines a polarization pattern under at least two different image acquisition states.

57. (Previously Presented) The optically readable data storage medium according to claim 53, wherein said set of optically readable characteristics which are randomly determined by a non-deterministic physical manufacturing process comprise a non-deterministic optical fluorescent pattern, wherein said illumination source and optical imaging sensor together determine a specific fluorescence characteristic of the fluorescent optical pattern.

58. (Previously Presented) The optically readable data storage medium according to claim 46, further comprising an authentication device, said authentication device comprising:

(a) an illumination source having a narrowband output adapted for exciting fluorescence at a wavelength differing from said narrowband output, having a time-varying polarization axis;

(b) an optical filter to exclude the narrowband output and pass the fluorescence at the wavelength differing from said narrowband output;

(c) an optical imaging sensor directed toward an imaging region, for sensing dichroic elements and a recorded data pattern through said optical filter; and

(d) a processor for extracting a pattern of dichroic elements from a background, based on changes in an output of said optical imaging sensor under a plurality of respective polarization axes, and for determining whether the extracted pattern corresponds to a predetermined pattern.

59. (Currently Amended) The optically readable data storage medium according to claim 46,

wherein said optically readable data storage medium comprises an optically readable substrate having a data pattern and a set of anisotropic optically readable fluorescent

characteristics which are randomly determined by a non-deterministic physical manufacturing process;

further comprising an authentication device, said authentication device comprising:

(a) an illumination source adapted for exciting the fluorescent characteristics;

(b) a polarizer;

(c) an optical filter which filters an output of the illumination source and passes the fluorescence;

(d) a common optical imaging sensor directed toward an imaging region, for sensing fluorescent characteristics and a recorded data pattern through said optical filter; and

(e) a processor for extracting a pattern of the anisotropic optically readable fluorescent characteristics, and for authenticating the storage medium based on a correspondence of the extracted pattern and the self-authenticating cryptographically processed set of identifications of the random optically readable characteristics associated with the data storage medium ~~recorded hash~~, whereby the data storage medium is resistant to reproduction and alteration of the data pattern can be detected.